C3.ai Digital Transformation Institute

Third Call for Proposals

AI to Transform Cybersecurity and Secure Critical Infrastructure

Introduction

The C3.ai Digital Transformation Institute (C3DTI) was established in March 2020 by C3 AI and Microsoft and co-led by the University of California, Berkeley (UC Berkeley) and the University of Illinois at Urbana-Champaign (UIUC), with consortium partners Carnegie Mellon University, KTH Royal Institute of Technology, Lawrence Berkeley National Laboratory (LBNL), Massachusetts Institute of Technology, Princeton University, Stanford University, and University of Chicago, and with high-performance computing support from LBNL and the National Center for Supercomputing Application (NCSA) at UIUC.

The goal of C3DTI is to catalyze cooperative research activities and advances in mathematical, statistical, and computing research, combining machine learning (ML), artificial intelligence (AI), the internet of things (IoT) and ethics and social responsibility in the development and deployment of technology. C3DTI is aimed at establishing fundamental scientific advances, algorithms, designs, and business change management practices to advance the science of digital transformation of societal systems.

C3DTI contributes to the new and emerging field of Digital Transformation Science by leveraging the personnel, laboratory, and research facilities at UC Berkeley, UIUC, and consortium partner institutions to form dynamic teams of the best researchers in the world to advance AI techniques for industrial, commercial, and public sector applications. This rich ecosystem helps address some of the most complex issues inherent in a massive societal digital transformation and build the foundation for a new science.

The purpose of this call for proposals is to solicit proposals for funding primary research to advance the science of AI and digital transformation in cybersecurity, with a focus on hardening information security (Infosec) and securing critical infrastructure.

It is anticipated that C3DTI will fund up to 20 research projects from this call for proposals. Collaborative multi-institutional collaborative proposals that exploit the Microsoft Azure Cloud and C3 AI Suite resources will receive preferential consideration. Initial results are to be reported within one year of award. All results of C3DTI-funded research accrue to the public domain under a NERF licensing model.

One-year awards will range from USD $100,000 to $1,000,000 in cash, in addition to high-performance supercomputing resources (HPC) and Azure Cloud and C3 AI Suite software resources.

AI to Transform Cybersecurity and Secure Critical Infrastructure

The pace, volume, and sophistication of attacks against our information infrastructure, networks, and our critical infrastructures are accelerating leading to substantive hacking, disruptions, and penetrations of our government, defense, and private sector information systems and energy, telecommunications, financial, water, and other critical infrastructures.

Advanced AI/ML techniques present an opportunity to bring new tools and methods to detect, explain, and respond to previously unknown attack vectors, leading to better security of IT systems, OT systems, and critical infrastructures.

Areas of interest to this call include but are not limited to:

1. AI techniques to identify previously unknown malware, ransomware, and zero-day vulnerabilities, enabling isolation and neutralization
2. AI-enabled network and system crawlers that can continuously search and identify persistent access mechanisms (backdoors), bots, remote access toolkits (RATS), stagers, and Trojans
3. AI forensics and attribution techniques to identify sources of attacks
4. AI techniques to automate simulated adversarial attacks to identify system and network vulnerabilities
5. AI techniques to accurately identify and enable the neutralization of phishing attacks
6. Change management techniques to prevent the weaponization of innocent insiders
7. AI techniques to detect the presence of advanced persistent threats and insider threats
8. AI-enabled network and/or system crawlers that access and continuously evaluate system security levels
9. AI techniques, perhaps in supervised or unsupervised learning, to provide early detection of system and/or network anomalies that might be indicative of unauthorized access, denial of service, or data exfiltration
10. Techniques and methods to enable the development of AI algorithms that are resilient to adversarial attacks
11. AI techniques to identify concentration risk in the software and computer supply chain
12. Change management to transform organizational behavior to manifest best practices in cyber hygiene
13. Techniques to respond to attacks at the organizational and societal level.

Eligibility

Proposal Principal Investigators (PIs) must be faculty researchers from C3DTI consortium partner institutions. Co-Investigators may be from C3DTI consortium partner institutions or other institutions. Preference will be given to proposals where the majority of the work and expenditures occur at C3DTI consortium partner institutions. C3DTI strongly encourages the submission of proposals that are interdisciplinary and inter-institutional across C3DTI consortium partner institutions as well as leading research institutions around the world. By submitting a proposal to this solicitation, proposal PIs and Co-Investigators agree to serve as reviewers for other proposals submitted to this solicitation.

Available Funding

It is anticipated that up to USD $10 million in Research Awards will be awarded from this Call for Proposals. C3DTI will also make available up to USD $2 million in Azure Cloud computing resources, supercomputing resources at UIUC's NCSA and LBNL's NERSC, and free, unlimited access to the C3 AI Suite hosted on the Microsoft Azure Cloud.

Proposals can request funding of USD $100,000 to $1,000,000 for an initial period of one (1) year. A simple budget is required as per the Proposal Preparation Instructions section of this document. Research Awards made from this solicitation must be used for direct costs only and no indirect costs or institutional overhead may be charged. There is a potential for an extension of the Research Award beyond the initial period of performance if needed with reasonable justification and approval. Preference will be given to proposals that include multi-institutional cooperation, coordination with private or public sector investigators, and exploit the utility of the Azure Cloud and C3 AI Suite resources provided.

Dissemination of Project Results

C3DTI encourages Research Award recipients to disseminate the results of their research during the award period in publicly accessible repositories, and more generally in the open literature for the public benefit. Such resulting publications should acknowledge the support of C3DTI. Research Award recipients are asked to provide technical reports during, and at the conclusion of the Research Award period. Due to the rapidly changing cybersecurity environment, Research Award recipients may be requested to provide additional information about their projects during the life of the Research Award.

Algorithms and Software Development

Proposals are required to use the C3 AI Suite (powered by Microsoft Azure) to show how the algorithms can be applied to real world data. Hence, proposals should explain how the C3 AI Suite and Microsoft Azure will be used to deal with new computational challenges and analyze complex data at scale. C3DTI will make cloud computing resources available to enable the utilization of the C3 AI Suite on the Microsoft Azure stack. C3 AI Suite capabilities include development and deployment of AI applications, data aggregation, and support for flexible REST interfaces. Also provided to Research Award recipients are C3 AI and C3DTI training materials on the use of the C3 AI Suite and computing platforms and technical support by C3DTI staff. Proposals that include a supercomputing requirement (e.g., large-scale data training or simulation) can be supported through scientific supercomputing resources contributed by UIUC's NCSA and LBNL's NERSC. Research Award recipients are strongly encouraged to share algorithms and software as open source for the public benefit. Proposers are strongly encouraged to consult with C3DTI technical staff on how they can leverage the C3 AI Suite and C3DTI computing resources to accomplish their proposed research. C3DTI will offer information sessions and scheduled office hours with technical staff, as well as make technical staff available to introduce proposers to the capabilities of the C3 AI Suite and the Microsoft Azure cloud computing and NCSA/LBNL scientific computing environments. Details of these events and contact information will be posted to the C3DTI website at https://c3dti.ai/.

Proposals should explain how the C3 AI Suite (powered by Microsoft Azure) will be used to deal with new computational challenges and analyze complex data at scale. To inform your proposal, you may review the following C3DTI video recordings that describe computing resources available to C3DTI awardees. An overview of the C3 AI Suite and supporting resources is at:

https://youtu.be/ES49oPY0EvQ?t=192

Further, a deeper dive into the capabilities of the C3 AI Suite is at:

https://www.youtube.com/watch?v=YIk0MfdOqGk

Additionally, the C3DTI Development Operations staff will be available to answer your questions about computing resources on Tuesdays beginning January 11, 2022 until the proposal submission deadline, between 12:00-1:00 PM U.S. Eastern / 9:00-10:00 AM U.S. Pacific. Please use this Zoom Meeting link:

https://illinois.zoom.us/j/81346993051?pwd=VnJwVkdBenZOZ0duWGxkOURJTytWdz09

No-cost, integrated technical support will be made available to select teams, whereby a C3DTI technical staff member is “embedded” with the Research Award recipient team to support and contribute to project work. Such arrangements should be jointly planned with the C3DTI technical team, which retains discretion and authority over selection of integration projects. These arrangements should be discussed before proposal submission and interested proposers should include details in the optional one-page description described in the Proposal Preparation Instructions section of this document.

Review Criteria

Projects will be peer-reviewed on the basis of scientific merit, prior accomplishments of the PI and Co-Investigator(s), the use of AI, machine learning, data analytics, and cloud computing, and the suitability for testing methods at scale. While all proposals are required to show how the C3 AI Suite and Azure will be used in their projects, no prior experience with C3 AI Suite and Azure is required. If proposers do not have prior experience with the C3 AI Suite and Azure, it is strongly encouraged that they consult with the C3DTI development operations staff for details on the functionality of the C3 AI Suite and Azure, and their help in addressing the computational challenges of their projects. Projects that leverage other sources of funding are welcome.

Proposal Preparation Instructions

All proposals should be submitted by the lead institution PI online via EasyChair at:
https://easychair.org/conferences/?conf=c3dticfp3

Proposals must be submitted to EasyChair by 11:59 PM PDT February 7, 2022.
Awards will be announced in March 2022 with a start date around June 1, 2022.

There will be an opportunity for the award winners to participate in the annual C3DTI Research Symposium to be held March 22-24,2022 in Miami, Florida, and formally receive the award.

Please use the Proposal Submission Template available in EasyChair when preparing your proposal. When finished, save your proposal in PDF format and upload all sections to EasyChair as a single PDF.

Proposals should use 11-point font and have 1" margins. The proposal structure and page limits are as follows, with additional instructions for each section provided below:

- Title Page: 1 page
- Project Description: 5 pages
- C3 AI Suite and Computing Platform Plan: 1 page
- Bibliography: 3 pages
- Key Personnel: 3 pages
- Budget and Budget Justification: 2 pages
- C3DTI DevOps Support (optional): 1 page

Title Page

Please include the following items:

- Full title of your proposed project
- Principal Investigator full name, title, affiliation, e-mail address, and phone number
- Co-Investigator full name(s), title(s), affiliation(s), e-mail address(es), and phone number(s)
- Lead Institution Authorized Organizational Representative full name, title, affiliation, mailing address, e-mail address, and phone number
- Lead Institution Grant Administrator Contact full name, title, affiliation, mailing address, e-mail address, and phone number
- Proposal Abstract (maximum 250 words)

Project Description

Please provide details about how your project will address each of the subsections below. Note that figures, tables, equations, etc. count toward the page limit.

- Project Relevance to AI to Transform Cybersecurity and Secure Critical Infrastructure
- Project Methodology
- Expected Research Accomplishments
- Criteria for Success
- Approach Novelty and Likelihood of Success
- Research Team Related Prior Accomplishments
- Computational Challenges and Resources Needed
- Suggested Reviewers

C3 AI Suite and Computing Platform Plan

Please provide a plan for how the C3 AI Suite tools and the Azure cloud computing platform will be used to solve the computational challenges on your proposed project.

Bibliography

Please provide citations to all references in your proposal. There is no set format for citations.

Key Personnel

Please provide a list of Key Personnel and brief (~100 word) biographical sketches for each person. Key Personnel should include the Principal Investigator, Co-Investigators, and other Senior Researchers. Links to full CVs for Key Personnel are allowed.

Budget and Budget Justification

Please provide a budget and a short (one page maximum) budget justification. Research Awards made from this solicitation must be used for direct costs only and no indirect costs or institutional overhead may be charged. The following budget items should be included:

- Research Personnel
  - This should include the cost and amount of time for faculty, students, postdoctoral scholars, and technical staff. Benefit costs are allowable.
- Administrative Support
  - A modest amount of project-related administrative support may be included if it is needed to conduct the proposed work. This should include the cost and time of administrative staff. Benefit costs are allowable.
- Travel
  - This should include travel-related expenses to disseminate the results of the research and collaborate with proposal partners.
- Materials and Supplies
- Other and Miscellaneous
  - This should include the cost and justification for any special equipment or needs.

C3DTI DevOps Support

This section is optional. If relevant, please provide information on expected requests for assistance from the C3DTI Development Operations (DevOps) staff on the proposed project.

Additional Resources and Contact

C3DTI will host a series of online information sessions in early January to provide an overview of the call for proposals and discuss the computing resources available to Research Award recipients as well as office hours with technical staff. Watch the official Call for Proposals webpage at https://c3dti.ai/research/ai-for-cybersecurity-and-critical-infrastructure/ for more details on these sessions as they become available.

Questions about general eligibility, proposal preparation, or research awards should be directed to the C3DTI by e-mail at proposals@c3dti.ai.